Combining System Safety & Reliability to Ensure NASA CoNNeCT's Success

Maria Havenhill, NASA Glenn Research Center
Rene′ Fernandez, NASA Glenn Research Center
Edward Zampino, NASA Glenn Research Center

Key Words: Hazard Analysis, Failure Modes and Effects Analysis, Limited Life Items List, Single Point Failure List, Integrated Approach.

SUMMARY & CONCLUSIONS

Hazard Analysis, Failure Modes and Effects Analysis (FMEA), the Limited-Life Items List (LLIL), and the Single Point Failure (SPF) List were applied by System Safety and Reliability engineers on NASA's Communications, Navigation, and Networking reConfigurable Testbed (CoNNeCT) Project. The integrated approach involving cross reviews of these reports by System Safety, Reliability, and Design engineers resulted in the mitigation of all identified hazards. The outcome was that the system met all the safety requirements it was required to meet.

1 INTRODUCTION

The National Aeronautics and Space Administration (NASA) is developing an on-orbit, adaptable, Software Defined Radio (SDR) and Space Telecommunications Radio System (STRS). It will be a test-bed facility on the International Space Station (ISS). The purpose of this test-bed facility is to conduct a suite of experiments to advance technologies, reduce risk and enable future mission capabilities on the ISS. The CoNNeCT Project will provide NASA, industry, other Government agencies, and academic partners the opportunity to develop communication, navigation, and networking technologies. The development of reliable space communication links is crucial to future NASA exploration missions. The current technology is based on reconfigurable, software defined radio platforms and the STRS Architecture.

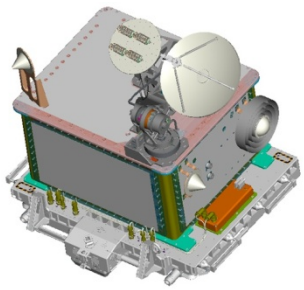

Figure 1: SCAN Testbed

The Nomenclature for CoNNeCT's on orbit system is the term "SCAN Testbed". This term is used to clarify the system which will actually be launched in 2012. (See Figure 1) [1]

2 CHALLENGES AND COMPLEXITIES OF CONNECT

A critical objective of CoNNeCT is to advance the Technology Readiness Level (TRL) for candidate spaceflight hardware and software. The CoNNeCT system is comprised of the flight system (which is the space based element) and the ground system (which is the terrestrial based element). The Flight System will launch on the H-II Transfer Vehicle (HTV-3), and be installed on the Express Logistics Carrier (ELC) 3 at the P3 truss location on the International Space Station (ISS). (See Figure 2)

The SCAN Testbed will be transferred and installed to the ELC via Extravehicular Robotics (EVR) activity. Extravehicular Activity (EVA) is the back-up. The Flight System is designed to operate for a minimum of two years.

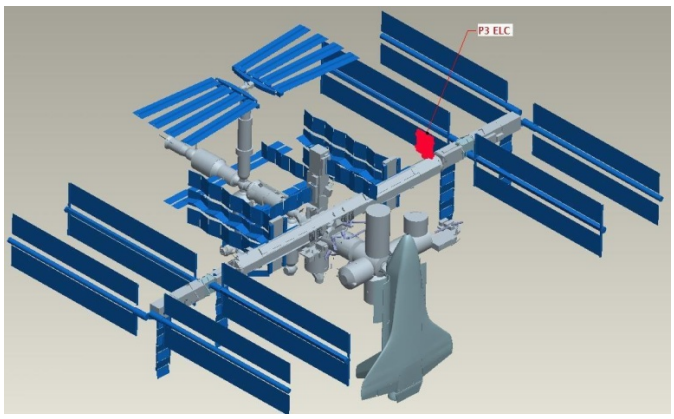

Figure 2: Location of SCAN Testbed Installed On ISS

What makes the application of safety and reliability techniques to CoNNeCT interesting is the intersection of constraints from schedule combined with the varied interests of the carriers (the HTV-3 and the ISS), the International Partners' systems impacted by CoNNeCT, and the concurrent definition of requirements that CoNNeCT has to meet, as well

as the combination of hardware and software providers supplying the components that make up the entire CoNNeCT flight system.

CoNNeCT began as a small, fast-track type project, where existing technology created for Lunar Robotic Orbiter (LRO) was utilized. An example of one of the technologies involved is the Traveling Wave Tube Amplifier (TWTA), a high power signal amplifier, that is an exact design copy of one used on the LRO. There are six difficult challenges for implementation of System Safety and Reliability on the CoNNeCT Project. They are the following:

1. Proto-flight development with an aggressive schedule constraint.
2. Accelerated building and test of flight hardware and software.
3. The number of International Space Station partners that will be impacted by the success or failure of CoNNeCT. These are: the Japan Aerospace Exploration Agency (JAXA), the Canadian Space Agency (CSA), the European Space Agency (ESA), and the Russian Federal Space Agency (RKA, commonly called Roscosmos).
4. Design requirements defining safe radio frequency (RF) limits for Ka-Band emissions were concurrently being developed by the ISS program.
5. The SCAN Testbed software is developed by five organizations: Glenn Research Center (GRC), Goddard Space Flight Center (GSFC); Jet Propulsion Laboratory (JPL); General Dynamics (GD), and Harris Corporation.
6. System coordination of hardware that together comprises the SCAN Testbed comes from GRC, GSFC, JPL, GD, Harris Corporation, and Sierra Nevada Corporation (specifically SpaceDev).

3 THE IMPORTANCE OF SAFETY AND RELIABILITY FOR CONNECT

This is a payload that will provide an opportunity for many investigators to explore the capabilities of radios that can change their signal configurations. That flexibility in signal configuration, combined with the ease of how the radio frequencies can impact so many other payloads, the ISS, and the visiting spacecraft vehicles, is the principle reason why system safety is so important.

The need for reliable future space communication links drives the visibility of the payload and makes it extremely important. The payload must function as advertised. As a result of its impact on so many different users on ISS, it is crucial that the payload meets the NASA reliability requirements as well as the safety requirements of all affected parties.

Utilizing reliability techniques ensures the payload will meet the planned mission objectives. Identifying points where the payload could suffer a single point failure allows the project to investigate alternate means where mission objectives could still be accomplished. Evaluation of the failure modes of various components and subsystems via the Failure Modes and Effects Analysis (FMEA) provides an understanding of how the components fail, the worst case effects of the occurrence of failure modes, and the causes of the failure modes. In particular, the FMEA identifies failure modes effects of very high severity: loss of payload mission, loss of payload hardware, and loss of life. These high-criticality failure modes overlap with the Hazard Analysis performed by System Safety engineers. Thus we pursued an integrated approach: System Safety and Reliability engineers conducted cross-reviews of the FMEA and Hazard Analysis, as well as integration of the data provided by the LLIL and the SPF list.

4 METHODOLOGY OF COMBINED APPLICATION

What will be briefly touched upon in this section are some examples of data from the reliability and safety assessments that were used to support each other.

At the beginning of the project development, application of system safety techniques, such as Preliminary Hazard Analysis (PHA), first identified the hazards associated with the system. Followed by Subsystem and System Hazard Analysis, this knowledge gave the project a map towards working solutions for either eliminating or controlling the identified hazards. The System Safety engineers also had to build upon their combined years of system safety expertise by learning the safety requirements and safety process for JAXA, since the payload would be transported on the HTV.

The hazard dealing with inadvertent release of RF energy is the most complex for the project and is the topic that required the most ingenuity from the System Safety and Reliability engineers. Control of this hazard involves identification of the range of the RF fields and their impact to stationary and non-stationary elements of ISS, as well as system control of the generated RF (how the system is turned on and off, and how accidental activation is prevented). Some of the RF limits for potentially impacted hardware and systems, especially for non-US property such as the Russian vehicles and the Canadian robotic arm, were not defined and made finding design solutions that would meet requirements very difficult. A few times, the project took their best guess and then had to work additional follow-on collaboration or even implement new design or operational changes to create closed solutions to these open problems. This iteration approach sometimes forced revisit of the safety and reliability work to ensure the new solutions did not invalidate positive findings on other parts of the project. The project's control of how the RF energy was generated and shut off is a combination of hardware and software design features, operational controls by both the ground support personnel and the on-orbit crew, and physical controls that are provided external to the SCAN Testbed itself.

A functional FMEA was developed for the project [2]. The Basic Failure Conditions considered were: premature operation; failure to operate within specification or at a prescribed time; failure during operation, including failure to contain or store energy; and failure to cease operation at a prescribed time. One identified failure mode from the

assessment was the Avionics Subsystem 1553 digital input/output (DIO) cards connector pins failing open or shorted to ground. The Critical Items List (CIL) that accompanied this FMEA had the 1553/DIO cards among the project's higher level identified failure modes. An example of how the System Safety and Reliability engineers increased their collective knowledge on this project is that during system-level testing, it was found that the DIO cards were the root cause of an uncommanded power-up of key components that are part of the control strategy to prevent the inadvertent release of RF energy. The failure was due to a design defect of the cards themselves (not related to the pins), and the project had to work with the manufacturer to obtain a design solution that would no longer create that issue. The solution was then presented to the Payload Safety Review Panel (PSRP) to demonstrate that the hazard would be controlled and that the project's inhibits were still valid.

Along with performing the FMEA, the LLIL/SPF document was prepared [3]. It became apparent that the flight system model design does not contain redundant subsystems based upon like-redundancy. However, alternative paths for success existed.

The Limited Life Items List was developed to identify hardware items that have an expected operating life or storage life that is less than the required operating life or storage life. Developing the list of Limited Life Items and a plan to address them was conducted fairly early in the design process in order to ensure reliable operation and mission success.

There was one safety critical limited operating life item identified - the Avionics Subsystem memory bank and associated software that are used to control the RF energy hazard. Taking into account the number of assumed use cycles per month against the need for a 2 year mission, the good bank availability, and a writing efficiency factor of 66%, the planned action and rationale was to accept the design as is since sufficient margin existed for life requirements.

Ground rules were established to help define what constitutes a single point failure and how it could be addressed. The CoNNeCT Project's interpretation of SPF with respect to the CoNNeCT project is complete loss of mission (e.g., that all radios completely fail). The design was evaluated for SPFs with the following ground rules:

- If a failed component can be fixed, it is not a SPF. Corrective maintenance action on the hardware is only applicable on the ground. On-orbit, corrective maintenance action is limited to software.
- An individual radio is not considered an SPF since the complete failure of one radio would not prevent the other 2 radios from operating.
- The Antenna Pointing System (APS) gimbal is not considered an SPF since the S-band to ground link can operate.
- The RF TX/RX system is not considered an SPF (including TWTA) because the L-band is available.
- Similarly, the entire RF system is not considered an SPF because the Ethernet link with ISS can still operate.

The analysis, with respect to the ground rules stated above, revealed that most SPFs are associated with the Avionics Subsystem. In addition to performing routing and processing on SDR data, the Avionics Subsystem is required to power all the other sub-systems.

The approach CoNNeCT has taken to address the SPF is to reduce the probability of an SPF occurring by using high reliability parts (the majority on the SPF List are Grade 2 or above). Where the Grade 2 parts quality cannot be maintained, extra attention was devoted to that component via a thorough environmental stress screening, derating, and burn-in testing. Infant mortality on lower grade components was minimized though the 100 hr burn in requirement being enforced on all SCAN Testbed hardware.

The results of all these assessments were vetted with the project and the system safety data was captured in safety data packages and presented to the PSRP. But there could have been additional refinement if the two disciplines' had further coordinated their findings. The system safety and reliability work was conducted by different individuals over time, with personnel leaving and joining the project and passing the responsibilities with each change. Each type of assessment, each view of the system, identified common issue areas such as the Avionics Subsystem. There were also areas that were identified as potential problems by one discipline's assessment but not the other's. An example is the hazard of not being able to maintain structural integrity over all expected loading conditions. This type of issue was not touched upon in the FMEA, the LLIL, or the SPF list since it was assumed the hardware would be designed to meet the requirements. In reality, this topic was the source of additional work and reverification/retest efforts when hardware provided by some of the third parties was found to be designed to the wrong structural loading requirements and had also been tested to the wrong verification loads.

5 DISCUSSION

The questions to ask are, "Were all hazards identified and mitigated? Has the system been designed and constructed to meet the mission requirements? Was all this activity effective?"

For the first question, the project has completed multiple flight safety reviews and ground/launch safety reviews, and multiple Technical Interchange Meetings (TIMs) and working meetings with the safety panels. All identified safety hazards have been mitigated. During hardware build-up and verification activities, new hazards arose based on hardware failures or as new data was obtained that concluded some hazards originally thought non-credible were now applicable. Additional work was required to determine impact and undergo resolution. The end result was that the project made the changes or worked issue resolutions with the proper authorities to ensure the system met all applicable safety requirements.

The second question, similar to the first, involved evaluation against the planned mission objectives. Through the multiple reliability assessments, potential weaknesses of

the system were identified and the rationale for how the system could either be modified, tested, or accepted as is was captured in the documentation. The story is complete of how the payload will meet the mission objectives of a 2 year life span as an external system on ISS and will provide multiple radio capability for investigators on Earth.

The final question's answer is derived from the answers to the first two questions. By being able to answer in the affirmative to the first two questions, one may say, "Yes, the system safety and reliability work was effective, since the system safety and reliability requirements were met."

6 FUTURE WORK

Launch of the HTV-3 is dependent on the ability of JAXA to respond to the recent earthquake and tsunami that occurred in March 2011. The launch was originally planned for January 2012, but has since been moved to a later date. But after the eventual shipment and launch of the flight system, the GRC SMA Organization will participate in a lessons learned session to discuss the effectiveness of the system safety and reliability effort. New items learned by the System Safety and Reliability team during the development of this project:

- JAXA safety design and process requirements
- RF limits for all ISS stationary hardware, visiting vehicles to ISS, on-orbit robotic equipment, and EVA crews
- ISS program processes for discussing and negotiating working solutions to system safety or reliability issues, especially if traditional solutions could not be implemented
- New failure modes for components and software (thus increasing the knowledge base of the system safety and reliability team)
- Difficulties that can occur when components and software for a system are provided by multiple parties – communication issues, subsystem integration problems under a tight schedule, and data needed for verifications not provided in a timely manner

This new information, coupled with capturing the experiences of working such a complicated payload with so many types of Design and System engineers, will provide the GRC System Safety and Reliability team with valuable data that can be shared with discipline coworkers and SMA professionals that become involved with similar projects and payloads.

REFERENCES

1. Maria Havenhill, "Flight Safety Data Package Phase III", GRC-CONN-SDP-0753, (Aug.) 2011. A NASA internal document.

2. Rene′ Fernandez, "FMEA (FAILURE MODES & EFFECTS ANALYSIS) / CIL (CRITICAL ITEM LIST)," GRC-CONN-ANA-0050, (Nov.) 2010. A publically available NASA internal document.

3. Rene′ Fernandez, "CONNECT Limited Life Items List (LLIL) and Single Point Failure (SPF) List," GRC-CONN-LIST-0147, (Apr.) 2010. A NASA internal document.

BIOGRAPHIES

Maria Havenhill
QE Division
MS 50-4 NASA Glenn Research Center
21000 Brookpark Road
Cleveland, Ohio 44135, USA

e-mail: MariaTheresa.A.Havenhill@nasa.gov

Maria Havenhill earned her MS degree in Mechanical Engineering/Business from Case Western Reserve University. Prior to December 2009 she was a support service contractor with SAIC. Work experience is primarily in the field of flight system safety, but other duties have included project management, risk management instruction and facilitation, quality assurance, and reliability. She assisted with the creation of an agency training curriculum for NASA safety and mission assurance professionals. Current projects other than CoNNeCT include Fault Tree Analysis of systems within the Multi-Purpose Crew Vehicle Program.

Rene′ Fernandez
QE Division
MS 50-4 NASA Glenn Research Center
21000 Brookpark Road
Cleveland, Ohio 44135, USA

e-mail: Rene.Fernandez-1@nasa.gov

Rene Fernandez earned his BS, MS, and did Doctoral work in Mechanical and Aerospace Engineering from Case Western Reserve University. Currently, he is the CoNNeCT SMA Team Lead at the NASA Glenn Research Center. Previously, he served as the GRC Reliability Engineer on the ASRG (Advanced Stirling Radioisotope Generator) project, and performed wind tunnel and flight research on air-breathing propulsion systems. Mr. Fernandez has published over 25 technical papers on the research he has been involved with.

Edward Zampino
QE Division
MS 50-4 NASA Glenn Research Center
21000 Brookpark Road
Cleveland, Ohio 44135, USA

e-mail: Edward.J.Zampino@nasa.gov

Edward Zampino earned his MS degree in Physics from The Cleveland State University. He worked as a Quality Assurance Engineer for the Technicare Division of Johnson & Johnson in the medical diagnostic instrumentation field. In 1987, he was able to join NASA, and to the present day, has supported many space flight and scientific research projects.